**Canada Response to the OHCHR Questionnaire – “The right to privacy in the digital age”**

1. **Overview**

Canada has a robust regime for protecting and respecting the privacy of individuals, as well as safeguards in place to ensure that Canada complies with its obligations under international human rights law.

Within Canada, privacy protections are enshrined in its Constitution, which guarantees the right to be secure against unreasonable search or seizure. Canada has a comprehensive legislative framework in place to promote and protect privacy, and is also actively addressing the privacy challenges of the digital age, most recently as a key component of its recently launched Digital Canada 150 strategy.

Canadian laws and policies pertaining to electronic surveillance ensure respect for individuals’ privacy, while providing for their safety and security. In the 2014 Speech from the Throne, a Parliamentary speech that sets out the broad goals and directions of the Government of Canada, the Government committed to respond to emerging threats “while ensuring Canadians’ fundamental privacy rights are protected.” In addition, Canada has independent and effective mechanisms to ensure Canadian national security organizations conduct their activities in accordance with their legal mandates, with ministerial direction and judicial oversight, as appropriate.

Canada is a State party to the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR prohibits interferences with privacy that are arbitrary or unlawful. Article 17 must be read in conjunction with Article 2 of the ICCPR, which establishes that State Party obligations under the Covenant apply to all individuals within its territory and subject to its jurisdiction.

With respect to the digital age, it is important to recall that the same rights that people have offline must also be protected online. Furthermore, privacy is intrinsically linked to other rights, in particular freedom of expression, including the freedom to seek, receive and impart information, as well as the freedoms of peaceful assembly and association. In any consideration of privacy in the digital age, it is important to take into account the interrelationship with these other rights.

1. **Canada’s Privacy Framework**

Canada has a robust constitutional, legislative, and administrative framework to ensure respect for and protection of individuals’ privacy rights, including in the context of digital communications.

***Canadian Charter of Rights and Freedoms***

Privacy rights are constitutionally guaranteed in Canada by the *Canadian Charter of Rights and Freedoms* (“the *Charter*”)[[1]](#footnote-1) . The *Charter* is Canada’s primary vehicle for ensuring that procedures, practices and legislation with implications for privacy rights are in accordance with Canada’s obligations under international human rights law.

Section 8 of the *Charter* guarantees that: “Everyone has the right to be secure against unreasonable search or seizure.” The purpose of this right is to protect against unjustified state intrusions on a person’s reasonable expectation of privacy. The privacy rights under section 8 extend to reasonable informational privacy interests, including in the context of digital communications and online activities more generally.[[2]](#footnote-2) Section 8 also restricts the sharing of individuals’ private information between government officials.[[3]](#footnote-3) The protection of a “reasonable expectation of privacy” is a normative standard, which allows constitutional privacy protections in Canada to evolve in line with changing societal values and technological realities. Where appropriate, Canada’s courts could take international standards into consideration when determining whether a state action has impermissibly intruded on a person’s reasonable expectation of privacy. As interpreted by Canada’s courts, section 8 of the *Charter* affords strong privacy protections in Canada, often beyond what is clearly required in international human rights law.

The *Charter* contains robust remedial provisions in the event of a violation. Where a government action is found to unjustifiably violate the *Charter*, courts can order an appropriate and just remedy, including an injunction, an order of compensatory damages, or the exclusion of unconstitutionally-obtained evidence from a court proceeding.

***Privacy Legislation in Canada***

Privacy rights are also protected by numerous statutory instruments. The *Privacy Act* sets out a code of fair practices for the collection, use, disclosure, and retention of personal information held by federal government institutions.[[4]](#footnote-4) The *Privacy Act* stipulates that collection is to be limited to personal information directly related to operating programs or activities, and must be justified by demonstrable need. It also provides individuals with a right of access to such information and a right to correction of their personal information. More than 250 Government institutions are subject to the Act. At the sub-national level, every Canadian province and territory has public privacy legislation, which governs the collection, use and disclosure of personal information held by government agencies.

*The Personal Information Protection and Electronic Documents Act* (PIPEDA)is Canada’s private sector privacy law that applies to commercial activities.[[5]](#footnote-5) The legislation was developed with input from businesses, governments, consumer associations and other privacy stakeholders. Private sector organizations are required to obtain the individual's consent when they collect, use or disclose personal information, except in some circumstances, such as information needed for an investigation or an emergency where lives or safety are at risk. The Act strikes a balance between an individual's right to the protection of personal information and the need of organizations to obtain and handle such information for legitimate business purposes and gives individuals the right to access, and request correction of, the personal information organizations have collected about them.

At the sub-national level, the provinces of Alberta, British Columbia, and Quebec have enacted comprehensive private sector privacy laws, which are recognized as substantially similar to PIPEDA and apply provincially. Additionally, several provinces have passed legislation to deal specifically with the collection, use and disclosure of personal health information by health care providers and other health care organizations.

***Digital Canada 150***

The government of Canada has recently unveiled its Digital Canada 150 strategy, which includes online safety and privacy among its key elements. A hallmark of the strategy is the newly proposed *Digital Privacy Act*, tabled in parliament on April 8, 2013, which provides for important improvements to PIPEDA aimed at strengthening the protection of personal information in the online environment. These include data breach notification requirements, changes to ensure businesses are able to use information to support their normal activities and improved compliance tools for the Privacy Commissioner of Canada.

As an important complement to Canada’s privacy legislation, Canada’s anti-spam law and regulations will protect consumers from spam and other threats that lead to harassment, identity theft and fraud. The legislation, which comes into force July 1, 2014, also contains measures against the collection of personal information through unlawful access to a computer and the unauthorized compiling or supplying of lists of electronic addresses. More information on Digital Canada 150 can be found at <http://www.ic.gc.ca/eic/site/028.nsf/eng/home>.

Related to the Digital Canada 150 strategy, the government of Canada has been proactive in encouraging individual Canadians to protect their privacy online. Launched in 2011, Get Cyber Safe is the Government of Canada’s national public awareness campaign. It aims to educate Canadians about Internet security and the simple steps individuals can take to protect their information and identity online. The campaign aims to bring together all levels of government and private sector to help Canadians be safer online. More information can be found at [www.getcybersafe.gc.ca](http://www.getcybersafe.gc.ca/).

***Criminal Code***

Part VI of the *Criminal Code* is one of Canada’s primary means for regulating electronic surveillance.[[6]](#footnote-6)  Part VI has two main objectives: to protect private communications by prohibiting their interception, and to specify the conditions in which an interception of a private communication may be authorized. At the heart of Part VI are the general prohibitions against willfully intercepting private communications, and against using or disclosing such communications. Subject to certain exceptions, these prohibitions bar third parties (including the police and other state actors) from intercepting private communications such as telephone conversations or emails. The key exceptions to the general prohibition on interception are when prior judicial authorization is granted on the basis of a legislative provision, or when one of the parties to the communication is consenting to the interception.

1. **Canada’s Safeguards to Ensure Ongoing Implementation of International Human Rights Obligations**

Canada has a number of safeguards to ensure that its procedures, practices, and legislation are in accordance with its obligations under international human rights law. Before deciding to ratify a human rights treaty, Canada will review its legislation, policies, programs, and practices for consistency. After ratification, there are various processes in place to review and facilitate effective implementation of Canada’s international human rights treaty obligations on an ongoing basis.

Canada’s international human rights obligations, including those related to privacy, are taken into account in the development of new legislation and regulations. Before tabling a Bill in Parliament, the government reviews the proposed legislation for consistency with human rights protections, including Canada’s international human rights obligations. Internal guidelines require that Cabinet be informed if any international agreements ratified by Canada have a bearing on the proposed legislation. In addition, guidelines instruct federal departments and agencies to respect Canada’s international obligations in their regulatory activities relating to a variety of areas, including human rights. Furthermore, Canada takes part in external processes such as periodic reviews by UN human rights treaty bodies and the UN Human Rights Council’s Universal Periodic Review.

To ensure that privacy implications will be appropriately identified, assessed, and resolved before implementing a program involving personal information, a federal government directive requires that federal institutions perform a privacy impact assessment for a new or substantially modified program or activity involving personal information. The privacy impact assessment is provided to the Office of the Privacy Commissioner, and the portion describing the risk area identification is made available to the public.

Training is available to federal officials on Canada’s international human rights treaty obligations, where relevant to their duties, to assist them in considering these obligations in their work.  Issues with respect to domestic or international human rights that are raised by the activities of a government department or agency can be referred to the Department of Justice for a legal opinion.

1. **Canada’s Independent and Effective Mechanisms for Ensuring Transparency and Accountability**

***In General***

The federal Office of the Privacy Commissioner is responsible for overseeing compliance of both the *Privacy Act* and PIPEDA.The Privacy Commissioner is independent of government, and reports directly to the House of Commons and the Senate. The Commissioner’s powers include: investigating complaints, conducting audits, and pursuing court action; publicly reporting on the personal information-handling practices of public and private sector organizations; supporting, undertaking, and publishing research into privacy issues; and promoting public awareness and understanding of privacy issues. At the sub-national level, provincial and territorial oversight is provided through either an independent commissioner or ombudsman authorized to receive and investigate complaints.

In addition to overseeing Canada’s two federal privacy laws, the Office of the Privacy Commissioner is also mandated under PIPEDA to educate the public about their privacy rights and organizations about their privacy obligations. In this role, the Commissioner undertakes various education and awareness initiatives and issues guidance to facilitate the implementation of PIPEDA and elaborate upon key aspects of the privacy obligations it contains.

Parliamentary committees also provide for transparency and accountability with respect to privacy. In particular, the House of Commons Standing Committee on Access to Information, Privacy and Ethics considers and reports to parliament on issues related to ethics and privacy. Parliamentary committees have undertaken studies related to new privacy challenges which result in reports being issued on specific issues (e.g., social media). The views of the federal Privacy Commissioner are frequently sought by parliamentary committees in the context of these studies and hearings, including those that relate to the challenges of law enforcement, the challenges introduced by digital communications and privacy considerations in the context of public safety interests.

***Canada’s National Security Organizations***

Canadian national security organizations conduct their activities according to their legal mandates, with ministerial direction and judicial oversight as appropriate. Each is subject to the scrutiny of the Privacy Commissioner, the Information Commissioner and the Auditor General. This is in addition to the rigorous oversight and review mechanisms that exist within Canada’s national security agencies.

With respect to the Communications Security Establishment (CSE), Canada’s cryptologic agency, all of their activities fully respect the legal parameters and authorities under which they operate in order to protect the privacy of Canadians. Under the *National Defence Act,* CSE is prohibited from directing its foreign intelligence or information technology security activities at Canadians anywhere in the world or anyone in Canada. The CSE Commissioner, independent of Government and of CSE, pursuant to the Commissioner’s legislative mandate, provides a robust review of the activities of CSE to ensure they are in compliance with the law and protects privacy. The CSE Commissioner also has the duty to hear public complaints and has all the powers of a Commissioner under Part 11 of the *Inquires Act*, including the power to summon witnesses to give evidence under oath. The CSE Commissioner is required by law to inform the Minister of National Defence and the Attorney General of Canada of any action by CSE which the Commissioner believes may not comply with the law, including the *Charter*, the *National Defence Act*, the *Privacy Act* and the *Criminal Code*. The Commissioner has never identified any actions of the CSE as being unlawful. The Commissioner’s annual reports to the Minister of National Defence and to Parliament can be found at <http://www.ocsec-bccst.gc.ca/ann-rpt/index_e.php>

With respect to the Canadian Security Intelligence Service (CSIS), their activities are conducted according to their legal mandate, under the *CSIS Act*[[7]](#footnote-7) *with* ministerial direction and judicial oversight, as appropriate. Moreover, judicial scrutiny is provided via a regime for the issuance of warrants by the Federal Court of Canada. CSIS is also subject to full and independent review by the Security Intelligence Review Committee (SIRC). SIRC is an independent, external review body which reports to the Parliament of Canada on the operations of CSIS to ensure that the powers given to CSIS are used legally and appropriately. SIRC is also mandated by law to report annually to the Minister of Public Safety and Emergency Preparedness who then presents the report to the Parliament of Canada. (SIRC Annual Report for 2012-2013 can be found at <http://www.sirc-csars.gc.ca/anrran/2012-2013/index-eng.html>).

With respect to the Royal Canadian Mounted Police (RCMP), their powers of interception are governed by Part VI of the Criminal Code, which sets out the procedures to obtain judicial authorization to conduct electronic surveillance of private communications for criminal investigations. These procedures are to be carried out to ensure that the privacy of individuals is appropriately respected during the surveillance. As an additional measure of accountability, section 195 of the Criminal Code requires the Minister of Public Safety and Emergency Preparedness to prepare and present to Parliament an annual report on the use of electronic surveillance under Part VI for offences that may be prosecuted by or on behalf of the Attorney General of Canada. (Latest report available at <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2012/index-eng.aspx)>

Furthermore, with the recent passage of Bill C-42 in June 2013, Enhancing Royal Canadian Mounted Police Accountability Act, the Government of Canada has bolstered the review of the RCMP through the Civilian Review and Complaints Commission for the RCMP, allowing greater access to RCMP information, enhanced investigative powers, and the ability to undertake policy reviews.

1. Part I of the *Constitution Act, 1982*, online: http://laws.justice.gc.ca/eng/const/page-15.html. [↑](#footnote-ref-1)
2. See e.g. *R. v. Morelli*, 2010 SCC 8, online: http://canlii.ca/t/28mrg; *R. v. Cole*, 2012 SCC 53, online: http://canlii.ca/t/ft969. Also, see generally *R. v. Dyment*, [1988] 2 SCR 417, online: http://canlii.ca/t/1ftc6; *R. v. Plant*, [1993] 3 SCR 281, online: http://canlii.ca/t/1fs0w. [↑](#footnote-ref-2)
3. See e.g. *R. v. Mills*, [1999] 3 S.C.R. 668 at para. 108 (“Privacy interests in modern society include the reasonable expectation that private information will remain confidential to the persons to whom and restricted to the purposes for which it was divulged.”), online: http://canlii.ca/t/1fqkl. [↑](#footnote-ref-3)
4. R.S.C. 1985, c. P-21, online: http://canlii.ca/t/524k6. [↑](#footnote-ref-4)
5. S.C. 2000, c. 5, online: http://canlii.ca/t/7vwj [↑](#footnote-ref-5)
6. R.S.C. 1985, c. C-46, online: http://canlii.ca/t/52668. [↑](#footnote-ref-6)
7. R.S.C. 1985, c. C-23, online: http://canlii.ca/t/7vdj [↑](#footnote-ref-7)